Legislative Audit Division

State of Montana

Report to the Legislature

May 1997

EDP Audit Follow-up

Montana State University-Bozeman

This report contains follow-up information on recommendations from an electronic data processing audit of Montana State University-Bozeman's computer center (95DP-01). Our initial recommendations addressed improving general controls over the university's electronic data processing environment. Of the 24 initial recommendations, 12 are implemented, 11 are partially implemented, and 1 is not implemented. Follow-up areas include:

- **Improving electronic access controls.**
- **Improving physical security controls and establishing formal contingency procedures.**
- **Improving overall documentation of controls and policies and procedures.**

Direct comments/inquiries to:
Legislative Audit Division
Room 135, State Capitol
PO Box 201705
Helena MT 59620-1705

97DP-03

EDP AUDITS

Electronic Data Processing (EDP) audits conducted by the Legislative Audit Division are designed to assess controls in an EDP environment. EDP controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States General Accounting Office.

Members of the EDP audit staff hold degrees in disciplines appropriate to the audit process.

EDP audits are performed as stand-alone audits of EDP controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

MEMBERS OF THE LEGISLATIVE AUDIT COMMITTEE

Senator Greg Jergeson, Vice Chairman
Senator Sue Bartlett
Senator Reiny Jabs
Senator Tom Keating
Senator Ken Miller
Senator Linda Nelson

Representative Ernest Bergsagel, Chairman
Representative Beverly Barnhart
Representative A. R. "Toni" Hagener
Representative Bob Keenan
Representative Robert Pavlovich
Representative Bruce Simon

LEGISLATIVE AUDIT DIVISION

Scott A. Seacat, Legislative Auditor
John W. Northey, Legal Counsel
Tori Hunthausen, IT & Operations Manager

Deputy Legislative Auditors:
Jim Pellegrini, Performance Audit
James Gillett, Financial-Compliance Audit

May 1997

The Legislative Audit Committee
of the Montana State Legislature:

This report is our follow-up review of our EDP audit (95DP-01) of Montana State University-Bozeman's internal controls relating to its computer-based applications. We reviewed recommendations relating to the university's general controls. This report contains implementation status of prior recommendations proposed for improving EDP controls at the department. Our prior recommendations included improving electronic access security, establishing formal contingency procedures, and improving overall documentation. Written comments from the department to our audit follow-up review are included in the back of the audit report.

We thank department personnel for their cooperation and assistance throughout the audit.

Respectively submitted,

“Signature on File”

Scott A. Seacat
Legislative Auditor

Legislative Audit Division

EDP Audit Follow-up

Montana State University-Bozeman

Members of the audit staff involved in this audit were Ken Erdahl and Alan Lloyd.

Table of Contents

Appointed and Administrative Officials

Board of Regents of Higher Education

Marc Racicot, Governor*

Nancy Keenan, Superintendent of Public Instruction*

Dr. Richard Crofts, Interim Commissioner of Higher Education*

		Term
		Expires
Jim Kaze, Chairman	Havre	1999
Patrick Davison, Vice Chairman	Billings	2000
Paul Boylan	Bozeman	1998
L. Colleen Conroy	Hardin	2001
Margie Thompson	Butte	2003
Ed Jasmin	Big Fork	2004
Mike Green, Student Regent	Missoula	1997

*Ex officio members

Commissioner of Higher Education

Dr. Richard Crofts	Interim Commissioner of Higher Education
Dr. Stuart Knapp	Interim Deputy Commissioner for Academic Affairs
Rod Sundsted	Associate Commissioner for Fiscal Affairs
Laurie O. Neils	Director of Budget and Accounting

Montana State University-Bozeman

Dr. Michael Malone	President
Robert M. Specter	Vice President for Administration and Finance
Dr. Thomas H. Gibson	Treasurer
Dr. Mark Sheehan	Director of Information Technology

Chapter I - Introduction and Background

Introduction

We performed a follow-up review of our electronic data processing audit (95DP-01) of Montana State University-Bozeman's Information Technology Center. The original report, issued in June 1995, contained 24 recommendations for improving existing controls within MSU-Bozeman's electronic data processing environment. This report outlines the status of the recommendations partially or not implemented.

Background on Original Audit

During our initial audit (95DP-01), we reviewed MSU-Bozeman's general controls as they related to the mainframe environment. We interviewed personnel to update our understanding of the hardware and software environment at MSU-Bozeman. We also reviewed available application documentation.

Follow-up Scope

Our original audit generated 24 individual recommendations. MSU-Bozeman concurred with 23 recommendations and partially concurred with one recommendation. The objective of our follow-up work was to determine the implementation status of the original audit recommendations. We reviewed agency documentation and interviewed staff to evaluate implementation of these prior audit recommendations.

Follow-up Results

Table 1
Implementation Status of Recommendations

Implemented	12
Partially Implemented	11
Not Implemented	1
Total Recommendations	24

Chapter II - Recommendation Status

Introduction

General controls are developed by the computer user to protect assets and limit losses. In our initial review, we found the general controls provide for controlled application processing on the mainframe computer system. We found hardware and system software, organizational and procedural controls to be adequate. However, we noted electronic access weaknesses which could compromise application data integrity. The physical security and system development weaknesses we identified could compromise MSU-Bozeman's ability to provide continuous processing services. In addition, we found several areas where documentation of controls and procedures is lacking, which could affect continuity and consistency of operations.

We determined the implementation status of the prior audit recommendations. This chapter discusses the status of each recommendation made in the initial report which are partially or not implemented.

Electronic Access Controls

Access controls provide electronic safeguards designed to protect computer system resources. Login IDs and passwords control access to MSU-Bozeman's operating system, computer programs, and data. System and application programmers have the highest degree of technical expertise in the computer facility and, therefore, play an important role in maintaining the application. However, application owners have primary responsibility for maintaining adequate controls. Without controls, inappropriate changes to programs and data may be concealed.

Proper access controls prevent and/or detect deliberate or accidental errors caused by improper use or unauthorized manipulation of data, programs, and/or computer resources. System security can limit access to specific areas. Limited access based on job duties prevents users from inadvertently or willfully executing programs or changing data unrelated to their job. System security is especially critical given the fact that MSU-Bozeman’s system is accessible, through modem and INTERNET, from nearly anywhere in the world.

Chapter II - Recommendation Status

We made 14 recommendations related to electronic access controls: 5 were implemented, 1 was not implemented, and 8 were partially implemented. The present status of those recommendations not fully implemented is discussed in the following sections.

Technical Support Staff Access Should be Limited

In **Recommendation #1** of the original report, we recommended MSU-Bozeman review the access privileges granted to users and restrict the "all" privileges to only those individuals who require it in the performance of their jobs.

The recommendation is partially implemented. In January 1997 MSU-Bozeman evaluated user IDs with high security ("all") privileges. In most cases, unnecessary "all" privileges were removed. However, in some cases, they have retained "all" privileges for individuals who don't require it, pending the design and implementation of an alternative access method.

"All" privileges allow the user, through various avenues, to circumvent security and potentially control the system. When users have these privileges, the operating system and service to others can be disrupted. Such disruptions can include failure of the system, destruction of data, and exposure of confidential information. For specific routines which require privileges, other access methods are available (such as using individual file access control lists (ACL)). Use of other methods would allow the individual to perform the required task without giving the user global privileges to the entire system.

Access to SYSTEM Account Should be Restricted

In **Recommendation #2A** of the original report, we recommended MSU-Bozeman restrict SYSTEM account access to the system administrator and the security officer.

Recommendation #2A is partially implemented. Access to the SYSTEM account allows individuals write access to everything on the system with no means of determining what changes are made by that individual. Previously, nine individuals had access to the SYSTEM account using a shared password. As of January 1997, seven individuals still have this access. MSU-Bozeman recognizes the importance of restricting access to the SYSTEM account. They have created a policy to restrict SYSTEM account access to the security officer and system administrator and are implementing the policy by migrating certain system administrative tasks away from the SYSTEM account. Personnel estimate they will need another 3 months to 1 year to fully implement the policy.

Access to the Audit Journal Should be Restricted

In **Recommendation #4A** of the original report, we recommended MSU-Bozeman restrict audit journal file access to the security officer and system administrator.

Recommendation #4A is partially implemented. Access to the audit journal is not fully restricted. In addition to the security officer and system administrator, five individuals assigned to the SYSTEM account have the ability to view and potentially modify the log. Staff assigned "BYPASS" privilege can view current log entries and potentially modify archived copies. Group access for operations staff and individuals with "SYSPRV" privilege is restricted. MSU-Bozeman created a policy to restrict SYSTEM account and BYPASS privilege access and is currently implementing this policy.

Access to Critical Application Files Should be Restricted

In **Recommendation #5A and B** of the original report, we recommended MSU-Bozeman restrict access to the critical application files to only those individuals needing it in the performance of their jobs, and log and review all access to the critical application files.

Recommendation #5A is partially implemented. System programmers still have unrestricted access to the application files. These files are critical to the operation of MSU-Bozeman's applications and data, and unlimited access exposes them to accidental or unauthorized change or deletion. MSU-Bozeman has documented their recognition of the risk and the need for programmer access to the application files. However, industry guidelines state access should be restricted. Programmers should perform their duties in a non-production test environment.

Recommendation #5B is partially implemented. In January 1997 MSU-Bozeman identified approximately 120 critical and/or sensitive system files. During the audit, MSU-Bozeman began, but had not completed logging activity to these files.

Programmer Access to Production Programs Should be Limited

In **Recommendation #6A and B** of the original report, we recommended MSU-Bozeman limit programmer access to production programs and data, and log and review all programmer activity relating to the production programs and data.

Recommendation #6A is partially implemented. Programmer access to production programs and data is not limited. MSU-Bozeman agrees with the recommendation but decided not to implement it due to inadequate staff resources. In addition to program maintenance, production support and ad hoc services, programmers have production control duties. MSU-Bozeman contends that additional FTE would be needed in order to separate production control and support functions. Efforts to document a full risk analysis is in process, and compensating controls have been identified.

Recommendation #6B is partially implemented. In January 1997 MSU-Bozeman identified all critical and sensitive production program and data files. Employees are creating security ACLs for all of these files, which will enable logging of programmer activity relating to these files.

Proxy Access Should be Restricted

In **Recommendation #7B and C** of the original report, we recommended MSU-Bozeman disable the INCOMING parameter for the main network, review all proxy logins and eliminate unnecessary proxy logins with privileges.

Recommendation #7B is not implemented. MSU-Bozeman has not disabled the "Incoming Proxy" parameter on the main network. Unless disabled, the “Incoming Proxy” parameter allows incoming proxies from other less secure systems to connect to the main network. This exposes the main network to remote access from a system with less restrictive security requirements, increasing the possibility of unauthorized access to critical data on the main network.

Recommendation #7C is partially implemented. In January 1997 MSU-Bozeman evaluated all proxy logins with privileges and documented their understanding of the risk, and the justification for use of these logins. By performing this review, MSU-Bozeman has taken steps to implement our prior audit recommendation. However, no logins with privileges were eliminated. Although use of proxy enhances use of security in some systems, security standards and industry guidelines state that proxy accounts should never be set up for a login ID with privileges that could damage the system.

Physical Security Controls and Other Issues

Physical security controls can improve the separation of custody over assets, prevent the accidental or intentional destruction of data, provide for the replacement of records that may be destroyed, and allow the continuation of operations following a major hardware or software failure.

We made 10 recommendations related to physical security controls and other issues: 7 were implemented and 3 were partially implemented. The present status of those findings partially implemented is discussed in the following sections.

MSU Should Improve Its Disaster Recovery Plan

In **Recommendation #9A and B** of the original report, we recommended MSU-Bozeman establish a detailed disaster recovery plan and test the plan.

Recommendation #9A is partially implemented. MSU-Bozeman has not established a formal disaster recovery plan. In March 1995 MSU-Bozeman started the process of developing a disaster recovery plan that will include all of the consolidated MSU campuses. MSU-Bozeman is currently defining all critical applications and hardware configuration specifications. MSU-Bozeman expects to complete and test formal disaster recovery procedures by Fall 1999.

Recommendation #9B is partially implemented. Once the disaster plan is complete, MSU-Bozeman plans to incorporate formal testing.

General Documentation

In **Recommendation #13** of the original report, we recommended MSU-Bozeman review present policies and procedures, and ensure critical processes are thoroughly documented to ensure continuity of operations.

The recommendation is partially implemented. In January 1997 MSU-Bozeman conducted a review of policies and procedures involving systems and facility security. MSU-Bozeman made modifications to existing policy, and are in the process of adding new policies for risk assessment, operating system documentation and employee termination. We reviewed internal memos and verified that work is progressing in development of new policies.

Summary

Overall, MSU-Bozeman has worked in strengthening the electronic access and physical security weaknesses which could compromise application data integrity and the ability to provide continuous processing services. In addition, there is improvement in documentation of controls and procedures which could affect continuity and consistency of operations.

MSU-Bozeman should continue work on strengthening electronic access and physical security weaknesses by fully implementing all prior audit recommendations.

Agency Response

MONTANA
STATE UNIVERSITY

Information Technology Center

MSU • Bozeman
P.O. Box 173240
Bozeman, MT 59717-3240

Telephone (406) 994-3042

April 22, 1997

RECEIVED
APR 23 1997

Tori Hunthausen
IT and Operations Manager
Legislative Audit Division
Room 135, State Capital Building
PO Box 201705
Helena, MT 59620-1705

Dear Ms. Hunthausen,

Enclosed please find our response to the Written Response Draft of your office's EDP audit of the Information Technology Center at Montana State University–Bozeman, which we received April 18.

Since last July, when I came to MSU–Bozeman, ITC has made strong, rapid progress toward meeting the recommendations of the 1995 audit. I'm gratified that your report reflects the many areas in which we have complied with those recommendations..

In the past few months I have enjoyed and learned much from my interactions with Alan Lloyd, Ken Erdahl, and you. The function your office performs is very valuable to the state and the university and you all carry it out with admirable professionalism.

It's been a pleasure working with you.

Sincerely,

Mark Sheehan, Director

Montana State University–Bozeman Information Technology Center

Response to Written Response Draft
EDP Audit Follow-up
conducted by
Legislative Audit Division
State of Montana

Recommendation 1. **The VAX/VMS "all" privileges should be reviewed and restricted only to those individuals who require it in the performance of their jobs.**

We concur with the present implementation status.

We are implementing individualized alternative access methods for users who previously had "ALL" privileges but who now require a subset of the privileges that "ALL" provides. Because this requires surveying the needs of each privileged user and modifying his/her access in specific, detailed ways, it is a time-consuming process. We plan to complete this work by August 1, 1997.

Recommendation 2A. **The VAX/VMS "SYSTEM" account should be restricted only to the system administrator and the security officer.**

We concur with the present implementation status.

We plan to complete implementation of this recommendation by August 1, 1997. It will require migrating some system administration tasks away from the primary system account, limiting use of that account only to those applications for which access is essential, and developing a mechanism for tracking the related activities of the individuals who use it.

Recommendation 4A. **Access to the VAX/VMS "audit journal" should be restricted only to the security officer and system administrator.**

We concur with the present implementation status.

Pursuant to recommendation 2A, access to the primary system account is being restricted. Pursuant to recommendation 1, "BYPASS" privileges (one of the "ALL" privileges) is being severely restricted. Our goal is thus to limit access to the audit journal to the security officer and system administrator by August 1, 1997.

Recommendation 5A. **Access to critical IA application files should be restricted only to those individuals needing it in the performance of their jobs.**

We concur with the present implementation status.

We have removed "ALL" privileges from the accounts of all administrative system programmers except the security officer and the system administrator. Some administrative system programmers still have duties that require that they work in the production control area under privileged accounts. Current staffing demands prohibit us from fully separating programming and production control duties. As staffing demands permit, we will move toward a more effective segregation of these duties.

Recommendation 5B. **Access to critical IA application files should be logged and periodically reviewed.**

We concur with the present implementation status.

We need to define precisely which individuals will have their activities logged under what circumstances. As stated, we have listed 120 sensitive data files whose access will be logged. By August 1, 1997 we will have established the list of programmers who require access to those files and will have modified access control lists for those files accordingly. At that point we will begin logging and reviewing all access to those files.

Recommendation 6A. **Programmer access to IA production programs and data should be limited.**

We concur with the present implementation status.

For the same reasons as in 5A, we have been unable to segregate program development and production control responsibilities. As staffing demands permit, we will move toward a more effective segregation of these duties.

Recommendation 6B. **All programmer activity relating to the IA production programs and data should be logged and periodically reviewed.**

We concur with the present implementation status.

We will complete application of security access control lists to the files mentioned in this recommendation by August 1, 1997.

Recommendation 7B. **The VAX/VMS "INCOMING" parameter for the main cluster should be disabled.**

We concur with the present implementation status.

The use of incoming proxies provides us with security benefits we value highly. Rather than disable this tool entirely, management has decided to enable incoming proxies only within a "trusted circle" of computers -- that is, we will allow a computer to accept proxies only from machines whose accounts ITC controls.

Recommendation 7C. **All unnecessary proxy logins with privileges should be reviewed and eliminated.**

We concur with the present implementation status.

We will have disabled incoming proxies from privileged accounts by January 1, 1998. It is first necessary to thoroughly review and test our system maintenance and production control activities to ensure that revoking privileged proxy logins does not result in costly service interruptions.

Recommendation 9A, 9B. **(a) A disaster recovery plan should be established according to the guidelines in the Montana Operations Manual, and (b) The plan should be adequately tested.**

We concur with the present implementation status.

As stated in the Written Response Draft, we expect to complete and test our formal disaster recovery plan by fall 1999.

Recommendation 13. **Present policies and procedures should be reviewed to ensure critical processes are thoroughly documented to help ensure continuity of operations.**

We concur with the present implementation status.

We will continue and expand the strong progress we have made to date in reviewing and revising our policies and procedures to reflect changing circumstances and needs.